Amendments to the Specification

Please replace the figure caption for Fig. 3b on page 7, lines 29 and 30, with the following rewritten figure caption:

Fig. 3b is a block diagram of a recovery scheme according to the embodiment of this invention shown in ~~Fig. 3b~~ Fig. 3a;

Please replace the paragraph beginning on page 11, line 17 and ending on page 11, line 31, with the following paragraph:

Access 224 to the valued content 200 by the purchaser system 220 is gained via a communication channel 210'. Depending on the particular method used to protect the valued content 200, the valued content 200 can be conveyed to the purchaser via the communication channel 210'. Preferably, communication channel 210' is the same as communication channel 210; however, other communications channels, such as wireless communication or digital cable television can also be used. In addition, in the case where the original digital file 212 is encrypted the decryption key or some authorization code can be conveyed to the purchaser system 220 by the communication channel 210' in which either the decryption key or the authorization code is embedded in [[it]] the digital string [[214]] 214'. In the latter case once the purchaser system 220 has access to the decryption key or the authorization code, the valued content 200 is then generated on the purchaser's system 220 (i.e. both the decryption of the original digital file 212' and the embedding 226 of digital string 214' in the original digital file 212').

Please replace the paragraph beginning on page 12, line 1 and ending on page 12, line 11, with the following paragraph:

An alternate embodiment of the present invention where the provider system 322 protects the valued content 300 by using a digital watermark containing the digital string 214 is shown as a simplified block diagram in ~~Fig. 3~~ Fig. 3a. In this embodiment, once the provider system 322 has obtained the digital string 214 from the purchaser system

220, the provider system 322 , utilizing watermark embedding process 350 generates [[a]] digital watermark [[350]] 356 from the information contained in the digital string 214 using a particular watermarking scheme. It is preferable that the provider system 322 utilize a watermarking technique that allows for the watermark to be retrieved regardless of the domain where it was embedded. This is important in applications such as audio and video and images requiring resilience to transcoding or change of format.

Please replace the paragraph beginning on page 12, line 12 and ending on page 13, line 4, with the following paragraph:

~~The~~ A watermarking embedding process 350 utilizes the digital string 214' as the watermark, original digital file 212' as the "cover" and an optional encryption key 334 to generate an encrypted digital watermark. The encryption key 334 may or may not be used depending on the particular application. In addition, the encryption key 334 may be used in combination with some unencrypted watermarks. Preferably the encryption key 334 used is of the type generally referred to as a private/public encryption key, and a combination of several keys are utilized to embed multiple encrypted digital strings 214'. The encryption key 334 provides additional security against manipulation or erasure by unauthorized parties trying to defeat the watermark. Preferably, in this embodiment, the modifications caused by the watermrk embedding process 350 are below a perceptible threshold that includes a criterion that weighs the value of the original digital file 212' against the loss resulting from unauthorized use. In addition, to further ensure robustness despite the small allowed changes; the information contained in the digital string 214' preferably is redundantly distributed over many samples (bytes, pixels, features, etc.) of the original digital file 212' shown as "n" in ~~Fig. 3~~ Fig. 3a. If "m" represents the number of different encryption keys used then "m" encrypted digital strings 214' are embedded in the original digital file 212' "n" times. This provides a global robustness, which means that the digital watermark can be recovered from a fraction of the watermarked digital file. These principles apply to watermarking techniques for various forms of valued content such as audio, images, video, formatted text, three-dimensional models, animation parameters, and others.

Please replace the paragraph beginning on page 13, line 5 and ending on page 13, line 17, with the following paragraph:

The output of the watermarking technique is the valued content 300, which contains the watermarked digital file. The valued content 300 is then conveyed 324 to the purchaser system 220 via the communication channel 210'. Preferably, the communication channel 210' is the same as the communication channel 210; however, other ~~communications~~ communication channels may also be used. Once, the purchaser or purchaser system 220 has obtained valued content 300 the purchaser has access to the digital information contained in the original digital file 212. An advantage of the present invention is that at the point the purchaser system 220 has access to the digital information the purchaser has a vested interest in ensuring that the information contained in the original digital file 212 is not distributed to other users since the valued content 300 also contains information about the purchaser, that has latent value to the purchaser.

Please replace the paragraph beginning on page 13, line 18 and ending on page 14, line 5, with the following paragraph:

A simplified block diagram of a watermarking recovery scheme is shown in Fig 3b, which provides additional incentive to the purchaser not to distribute the valued content ~~300~~ to other users. The provider system ~~322~~ 322', when the valued content 300 is conveyed 324 to the purchaser system 220 (as shown in Fig. 3a), also places in the public domain a subset of the "m" versions of the public encryption keys of the private/public encryption key 334' used and makes this known to the purchaser at the time of purchase. The provider system ~~322~~ 322' also makes a watermark extraction process publicly available. Thus, if the purchaser then either distributes the valued content 300 directly to others or the purchaser attempts to disable the digital watermarking resulting in a possibly distorted digital file 301 and then distributes the possibly distorted digital file 301 to others, the subsequent users 351 can gain access to the very information that the purchaser wants to keep private by utilizing the public encryption key of the private/public encryption key 334' distributed by the provider

system 322. The watermark extraction process 352 using the public encryption key of the private/public encryption key 334' extracts bits of information (i.e. the digital string 214") from either the valued content 300 or the possibly distorted digital file 301. Preferably, the provider system 322 distributes the public encryption key over the Internet, however other communication channels may also be used without diminishing the utility of the present invention.

Please replace the paragraph beginning on page 14, line 6 and ending on page 14, line 18, with the following paragraph:

In addition, the provider system 322' can also extract the digital string 214" from either the valued content 300 or the possibly distorted digital file 301 by utilizing either the encryption key of the private/public encryption key 334' or the watermark/original digital string 350'. Thus, by utilizing both a combination of the private/public encryption keys 334' and redundantly distributing the digital string 214' over numerous samples in the valued content 300, the provider system 322 gains the advantage of providing an additional incentive to the purchaser not to unlawfully distribute valued content 300. Furthermore, by utilizing the public encryption key of the private/public encryption key 334' the provider system 322 can also maintain one or more of the redundantly embedded digital strings 214' in a secure manner for eventual decryption (i.e. using the private encryption key of the private/public encryption key 334'), identification, tracking, and enforcement of the owner's legal rights against those who have improperly distributed the valued content 300.

Please replace the paragraph beginning on page 14, line 19 and ending on page 14, line 30, with the following paragraph:

An alternate embodiment of the present invention, where the provider system 422 protects the valued content 400 by generating a steganographic object containing the digital string 214, is shown as a simplified block diagram in Fig. 4. In this embodiment, similar to that shown for watermarking in Figs. 3a-3b, the provider system 422, utilizing a steganographic generation process 455, generates, from the digital file

212', the digital string 214', and a random number generator 444, a steganographic object 456 using a particular steganographic technique. In this embodiment, it is also advantageous to use a private/public encryption key 434 and to hide the information contained in digital string 214' multiple times denoted by "n" in Fig. 4. Preferably, the provider system 422 distributes the public encryption key over the Internet, however other communication channels may also be used without diminishing the utility of the present invention.

Please replace the paragraph beginning on page 16, line 5 and ending on page 16, line 11, with the following paragraph with the following paragraph:

The encrypted digital file is conveyed 524 over communication channel 210' and can be distributed via CD-ROM, or the Internet, but may also include other communication channels such as networks, digital cable TV, etc. This embodiment is particularly applicable to those media that makes the information available on a public basis. For example, mass mailings of CD-ROMs to potential customers whose names are selected from a target mail list.

Please replace the paragraph beginning on page 16, line 29 and ending on page 17, line 18, with the following paragraph with the following paragraph:

The provider system 522 also gains the advantage of providing an additional incentive to the purchaser not to unlawfully distribute the purchaser authorization file 546 by utilizing both a combination of the encryption keys 534 and redundantly distributing the encrypted digital string 514 numerous times in the key 547. In addition, when the provider system 522 uses a private/public encryption key the provider system 522_a by encrypting with the public key 534_a can also maintain one or more of the redundantly embedded encrypted digital strings 514 in a secure manner for eventual identification, tracking, and enforcement of the owner's legal rights against those who have improperly distributed the purchaser authorization file 546. The provider system 522 also places in the public domain one or several versions of the public encryption key 534 and makes this known to the purchaser at the time of purchase. If the purchaser

then distributes the purchaser authorization file 546 to others the subsequent users can gain access to the very information that the purchaser wants to keep private by utilizing the public encryption key 534 distributed by the provider system 522. The public encryption key extracts bits of information (the digital string 214) from the purchaser authorization file. Preferably, the provider system 522 distributes the public encryption key over the Internet commonly referred to as the world wide web 535, however other communication channels may also be used without diminishing the utility of the present invention.

Please replace the paragraph beginning on page 20, line 29 and ending on page 21, line 10, with the following paragraph with the following paragraph:

The digital processing system also contains an interface 788 allowing the provider system 722 to communicate with the content ~~owners system~~ owners' systems 761 and 761' as well as the ~~purchaser~~ purchasers' systems 720 and 720' over the communication channels 210. Preferably, the communication channel 210 is a digital network 772 such as what is commonly referred to as the Internet. Other communication channels such as wireless communication, wireline telephone, digital cable television, as well as other point-to-point, point-to-multipoint, and broadcast communications methods can also be used. The communication channels 210 can also include various combinations of the above mentioned channels. For example, the provider system 722 and the content owner system 761 can communicate over a wireless communication channel and the provider system 722 and the purchaser system ~~220~~ 720 can communicate over a wireline telephone channel.

Please replace the paragraph beginning on page 21, line 11 and ending on page 11, line 23, with the following paragraph with the following paragraph:

Also shown in Fig. 7 is a digital processing system 790 that contains a processor ~~786~~ 796, storage 794 and a content perceiver 792 that is all used by the purchaser system ~~220~~ 720 for generating the digital string 214 and accessing the valued content 200 shown in Fig. 2. For example, the processor 796 decrypts the encrypted digital file

412 shown in Fig. 5. The content perceiver 792 is any device necessary to perceive the original data file 212 shown in Fig. 2 and may be more specialized than the content perceiver 782 used by the provider system 722. Storage 794 can be processor memory, other computer memory such as a hard disk or portable memory such as a CD-ROM, DVD, DAT etc. or any appropriate combination. The interface 798 allows the purchaser system 720 to communicate with the content owner systems 761 and 761' as well as the provider system 722 over the communication channels 210.

Please replace the paragraph beginning on page 21, line 11 and ending on page 11, line 23, with the following paragraph with the following paragraph:

The point of sale machine 774 also shown in Fig. 7 provides several advantages. It is applicable when purchaser system 220 does not have either interface 798 or access to communication channel 210 but has the other equipment necessary to access valued content ~~100~~ 200 as shown in Fig. 2. In this embodiment communication channel 710 preferably is a digital network such as what is commonly referred to as the Internet. Other communication channels such as wireless communication, wireline telephone, digital cable television, as well as other point-to-point, point-to-multipoint, and broadcast communications methods can also be used. In addition, the use of the point of sale machine 774 is also applicable where purchaser system 220 wants to purchase valued content ~~100~~ 200 as shown in Fig. 2 in a form which is useable in a portable media format such as DVD or DAT. Further, it is also applicable when it is advantageous to the provider system 722 not to share extrication program 572 and/or digital string embedding program 570 or key 547 with purchaser system 220, as shown in Fig. 5, since in this case the purchaser obtains valued content ~~100~~ 200 with digital string 214' already embedded.

Please replace the paragraph beginning on page 23, line 9 and ending on page 23, line 21, with the following paragraph with the following paragraph:

The provider system also determines what if any provider information should also be embedded in the digital file before conveying the digital file to the purchaser in

step 808. This provider information can be, for example, a reward or finders fee that adds further protection to the provider that the purchaser will not unlawfully distribute the digital file. The provider system, in step 810, determines the redundancy levels "n" and " n' " where n is the number of times the purchaser information acquired in step 804 will be embedded into the digital file accessed in step 800. The value " n' " is the number of times the provider information determined in step 808 will be embedded into the digital file accessed in step 800. In determining the value of both "n" and " n' " the provider may take into consideration the purpose and value of the digital file, the attributes of the digital file for both watermarking and the steganographic technique being utilized as well as others.